AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Preetham C. Rao, Special Agent of the Federal Bureau of Investigation, United States Department of Justice, hereinafter referred to as Affiant, being duly sworn under oath, hereby deposes and states as follows:

INTRODUCTION

1. Affiant is an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7) and Federal Rule of Criminal Procedure 41(a)(2)(C), as a Special Agent (SA) of the Federal Bureau of Investigation (FBI). Affiant is empowered to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516.

2. Your affiant has 17 years of law enforcement experience. I have been employed with the FBI since October 2005 and have been a Special Agent since February 2009. I have been assigned to the Cleveland Division since September 2018. During my tenure, your affiant has been assigned to investigations involving Public Corruption, Fraud against the Government, Counterterrorism, and Civil Rights. Your affiant has also been assigned to and supervised matters pertaining to Violent Crimes Against Children. Your affiant is presently assigned to the FBI Cleveland Division where I am the Crimes Against Children Coordinator. Your Affiant has received specialized training at the FBI Academy in Quantico, Virginia, on how to investigate a variety of Federal criminal violations. Your affiant is trained on conducting surveillance, conducting electronic and physical searches, and interview and interrogation techniques. Your affiant has received additional

specialized training in child sexual abuse and cyber investigations including the use of social media, Internet Protocol (I.P.) Address tracking, use of chat rooms and the dark web.

3. Between Affiant's work experience and training, Affiant has either taken part in, assisted in, or received extensive training in all of the usual methods of investigation, including, but not limited to, physical surveillance, analysis of evidence, the execution of search warrants resulting in the seizure of drugs, and the monitoring of court ordered Title III wiretaps.

4. I have probable cause to believe that evidence of a crime, fruits of a crime, contraband and instrumentalities of violations of: 18 U.S.C. § 2423(a) (Transportation with Intent to Engage in Criminal Sexual Activity); and 18 U.S.C. § 2252(a)(4)(B) (knowingly possess child pornography) are located within 14567 Madison Avenue #204 Lakewood, Ohio 44107 (hereinafter the "SUBJECT PREMISES"). The SUBJECT PREMISES was occupied by and presently stores electronic equipment used by GARETH SCHAKEL (hereinafter SCHAKEL).

5. I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, as further described in Attachment A, and incorporated herein by reference, which is in the Northern District of Ohio. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to transportation of a minor with intent to engage in illicit sexual conduct and possession of child pornography. I request authority to search the entire SUBJECT PREMISES, including the residential

dwelling and any computer, computer media, and mobile computing device located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime

6. The statements contained in this affidavit are based in part on information developed by other Special Agents and Task Force Officers of the FBI and county-level officials who have participated in the investigation. Unless otherwise noted, whenever in this affidavit your Affiant asserts that a statement was made, the information was provided by another law enforcement officer or an investigator (who may have had either direct or hearsay knowledge of the statement) to whom your Affiant has spoken or whose report your Affiant has read and reviewed. Likewise, any information pertaining to personal data on subjects and records checks, has been obtained through the Law Enforcement Automated Data System (LEADS), various state driver's license motor vehicle records, online database searches or the National Crime Information Center (NCIC) computers, various open-source databases such as CLEAR and LexisNexis, and public social media websites such as Facebook and Instagram. Not all facts of the investigation have been included. Only such facts as to establish probable cause are outlined herein.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

7. The following definitions apply to this Affidavit:

   a. "Element" is a free and open-source United Kingdom-based instant messaging application that supports end-to-end encryption, private and public groups, sharing of files between users, voice and video calls, and other collaborative features with help of bots and widgets. It is available as a web application that is

through any modern web browser, as desktop apps for Windows, Mac, and Linux, and as a mobile app for Android and iOS (the operating system used on Apple devices). Element uses the "Matrix" protocol (defined below).

b. "Matrix" is an open standard and communication protocol for real-time communication. It makes real-time communication work seamlessly between different service providers, in the way that standard Simple Mail Transfer Protocol email currently does for store-and-forward email service, by allowing users with accounts at one communications service provider to communicate with users of a different service provider via online chat, voice over IP, and video telephony.

c. "Discord" is a social media communication platform that is used by tens of millions of people to communicate with voice calls, video calls, text messaging, sending media and files in private chats or as part of communities called "servers."

d. "Omegle" is a free online chat website that allows users to socialize with others without the need to register. The service randomly pairs users in one-on-one chat sessions where they chat anonymously using the names "You" and "Stranger." The parties may interface via written chat or choose face to face.

e. "Snapchat" is a social media communication platform and mobile application that is used by tens of millions of people ages 13 or over (as claimed by the user) that allows users to send and receive "self-destructing" photos and videos as well as allowing users to communicate via chat. Photos and videos are sent from one

person to one other person, from one person to a group of people, or one person to post their "story" for all their friends to view, depending on the privacy settings of the specific user. Chat messages can also be sent from one user to another user or from one user to a group of users.

f. "Computer server" or "Server", as used herein, is a computer that is attached to a dedicated network and serves many users and is designed to provide shared resources and services to users on the network. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A DNS (domain name server), in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.google.com, into his or her web browser. The domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

g. A Mobile Messaging Application is an application used on mobile devices, including phones, tablets, and others, that allows users to communicate with other users via text; some also allow voice and video calling. Some of these mobile messaging applications provide end-to-end encryption. This means that the communications from one user to another are unreadable to anybody outside of the conversation, including the owner of the mobile messaging application. In these instances, having direct access to the device with the mobile messaging application or having access to the account on the mobile messaging application

that was used to send and receive messages is the only way to be able to view encrypted conversations.

h. "Mobile computing devices," are handheld electronic devices used for storing data (such as names, addresses, music, photographs, appointments or notes) and utilizing computer programs. Some mobile computers also function as wireless communication devices and are used to access the Internet and send and receive e-mail. Mobile computers often include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Many users of these devices also use cloud storage applications to store data such as images and videos in order to back up data, duplicate data in order to access data from other devices, or to free up space on their device. Most mobile computers run computer software, giving them many of the same capabilities as personal computers. For example, mobile computers users can work with word-processing documents, spreadsheets, presentations, Internet browsing and chat applications. Mobile computers may also include global positioning system ("GPS") technology for determining the location of the device. Mobile computing devices include, but are not limited to, laptops, tablets and smartphones. This type of Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and a mobile computer. As the amount of data that people store on their mobile

devices has increased, smartphones and other mobile computing devices are also commonly synched with, or connected to, a desktop or laptop computer for backup data storage. This allows users to access selected data, such as photos, emails, contacts and documents, across multiple devices, or to recover this data if their mobile device is broken or lost.

i. A "wireless telephone" (or mobile telephone, cellular telephone, or smartphone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

j. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

k. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, by any means, relevant to the statutes outlined above in paragraph 4. Also, passwords, encryption keys, or other applications necessary to access computers, computer servers, mobile electronic devices, and electronic storage devices may be stored by electronic or manual means. Electronic storage including but not limited to thumb drives, flash drives, hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, or optical disks. Manual storage would include but not be limited to paper or another surface such as a chalkboard, wall, or desk).

FACTS AND CIRCUMSTANCES REGARDING PROBABLE CAUSE

8. On March 29, 2023, fifteen-year-old fifteen-year old minor victim (hereinafter "MV") was reported missing to the Davidson County, North Carolina Sheriff's Office by her mother. On this day, MV was observed on home security video leaving her Thomasville, North Carolina residence. MV aimed the security camera down toward the porch floor, flashed a peace sign with her hands to the camera, and walked away. MV left a letter in her kitchen saying goodbye, giving items to siblings, apologizing to the family, and stating she was safe. MV did not possess a cellular phone but departed with a Dell Latitude laptop 5500.

9. On April 06, 2023, MV was recovered in Pennsylvania from a car driven by ELLIJAH DEANDRE KENNEDY (hereinafter KENNEDY). Investigators found a used condom and pregnancy test during a search, pursuant to a search warrant, of KENNEDY's

residence. KENNEDY has since been arrested and faces charges in the Eastern District of Pennsylvania.

10. During a forensic interview after her recovery, MV disclosed that KENNEDY had picked MV up at her North Carolina home, and transported her to his home in Bristol, Pennsylvania. During a weeklong stay, KENNEDY made MV take sexually explicit photographs of herself at his apartment. KENNEDY then sent those photographs to himself and a friend using Snapchat. KENNEDY met MV on the online text and video chatting application, Omegle, and KENNEDY introduced MV to a messaging application called Element. MV reported that, prior to KENNEDY's travel to North Carolina to pick her up, she told KENNEDY that she was 15 years old, and he told her that he was 18 years old. (KENNEDY was actually 28 years old.) In her forensic interview, MV claimed that she could not remember whether she engaged in sexual contact with KENNEDY while at his residence in Pennsylvania. In a subsequent handwritten note to her mother, MV later disclosed that she did, in fact, have sexual contact with KENNEDY on several occasions while at his residence.

11. During early stages of the investigation into MV's disappearance, Investigators in Davidson County, North Carolina gained access to MV's school profile through Davidson County school officials. Davidson County investigators then remotely logged into MV's account making her web history, logins, usernames, and passwords accessible. As a result, investigators observed MV possessed several usernames for Element.

12. On April 3, 2023, Davidson County created an Element user account called "testdummy2511" and accessed a public Element forum. The forum was called

"#General:kitsunet.info." There, investigators observed a posting from MV approximately two to three days prior to her departure and saw evidence of her moving to a private forum.

13. Local authorities screen-recorded the content of the public Element forum and noted eight other users besides MV (whose account name was "bunny_bunss:kitsunet.info").

Display Name	Account Name
Broc	@adamohio2022:kitsunet.info
gartral	@gartral:kitsunet.info
Teknikal_Domain	@teknikal_domain:Matrix.TDStoragebay.com
KE8RMV/M	@KE8RMV:info
bun buns	bunny_bunss:kitsunet.info
Austin Huang	@austin:tchncs.de
SilverWereWolf	@Silverwerewolf:anontier.nl
Cugai	@cugai:kitsunet.info
SCHAKELhammer	@SCHAKELhammer:kitsunet.info

14. Investigators queried a publically available domain research website for the domain "kitsunet.info" that identified GARETH SCHAKEL (SCHAKEL) as the administrator:

Name:	Gareth Schakel
Street:	14567 Madison Avneue #204
City:	Lakewood

State/Province:	Ohio
Postal Code:	44107
Country:	US
Phone:	440-947-0464
Email:	Gareth7yo@gmail.com

15. A criminal history check reflected that SCHAKEL was a Tier II registered sex offender[1] and on active community control (i.e. parole) and under the supervision of the Ohio Adult Parole Authority.

16. On the evening of April 4, 2023, the Cleveland Office of the FBI and the Ohio Adult Parole Authority located SCHAKEL at SUBJECT PREMISES[2]. Adult Parole Authority took SCHAKEL into custody for investigation of violation of his post release control. North Carolina FBI conducted a mirandized interview in which SCHAKEL confirmed being the administrator for the Element group of which MV was a member. SCHAKEL conveyed that the server was located in the closet of his mother's condominium (SUBJECT PREMISES).

17. The location was corroborated by FBI Agents who searched SUBJECT PREMISES for MV pursuant to consent from SCHAKEL's mother, KATHRYN SCHAKEL (hereinafter KATHRYN), who lived there. Specifically, in the closet of the back bedroom at the end

[1]In March 2011, Schakel was convicted for pandering sexually oriented material and possessing criminal tools.
[2] As a registered sex offender, SCHAKEL is not permitted to live at the SUBJECT PREMISES, since it is located too close to a school. However, SCHAKEL spends the majority of his time there but sleeps at a homeless shelter at night.

of the hallway, one FBI Agent observed a closet containing numerous computer towers on racks. Wires flowed out from the closet to another tower on the floor of the bedroom. A different Agent observed a computer in the family room.

18. SCHAKEL explained that he migrated to Element after he grew disenchanted with Discord, the application he formerly used to communicate with others including his mother and a friend named ADAM DAVIS (hereinafter DAVIS). Records checks reflected that DAVIS too was a registered sex offender[3].

19. SCHAKEL told investigators that MV was already a member of Element and he had invited her to join his Element group. In one instance, SCHAKEL claimed that MV sent a nude, sexually explicit photo on Element. SCHAKEL did not know MV's age but claimed he admonished MV that his group was not the appropriate platform for such content.

20. Meanwhile, on April 5, 2023, investigators located DAVIS who consented to a mirandized interview as he was in the custody of the Adult Parole Authority. When advised that law enforcement was seeking a missing girl, DAVIS volunteered that he might know whom she was. DAVIS correctly identified MV among a selection of three unmarked colored photographs.

21. DAVIS conveyed that he met SCHAKEL in prison. The two men maintained contact after leaving state custody. DAVIS described SCHAKEL as technically literate and advised that SCHAKEL operated his own computer server and chat platform called Element from his late father's home in Lakewood, Ohio.

[3] DAVIS was convicted of unlawful sexual conduct with a minor; importuning; and possessing criminal tools.

22. DAVIS conveyed being invited to an Element chat room created by a user named "BUN BUNSS." DAVIS stated that SCHAKEL told him that he first met BUN BUNSS in a fetish chat room on another platform and invited her to Element. Once there, BUN BUNNS initiated her own chat room within Element where only four users were present: BUN BUNSS [MV], gartral [SCHAKEL], teknickol [unknown user], and brock [DAVIS]. Within this Element group chat, MV shared approximately 15 photographs of herself that were "selfie" in nature in which she was in various stages of undress, nude, or were pornographic. MV's face was visible in some of the images. Text surrounding the images was sexual in nature and described the sex acts the users wanted to engage in with MV. DAVIS stated he did not know BUN BUNSS' true identity or age but admitted BUN BUNSS spoke at length about her academic troubles in high school and referenced living with her parents.

23. DAVIS went on to say that MV, SCHAKEL, and DAVIS were in a separate Element chat room together. Within this chat room, MV also shared numerous pornographic images of herself. In fact, SCHAKEL created the private room because MV was showing her face in many of these pictures.

24. After MV went missing, SCHAKEL told DAVIS that MV was in Pennsylvania with an unknown man that she had met years prior on an unknown platform. SCHAKEL also told DAVIS that MV had needed to depart her home very quickly, leaving all of her belongings behind, and that the unknown man she was with provided her a laptop and cellular phone in exchange for "blow jobs." DAVIS did not know how BUN BUNSS got to Pennsylvania, but opined that the man probably drove to get her. The last

communication DAVIS had about the girl was on or about March 31, 2023 when SCHAKEL told DAVIS she was in Pennsylvania.

25. On April 6, 2023, DAVIS consented to a follow up mirandized interview where he conveyed SCHAKEL and BUN BUNSS were linked romantically, however, he did not know the extent of their relationship. DAVIS surmised that SCHAKEL's relationship with BUN BUNSS was based upon the idea that SCHAKEL was the dominant partner in their relationship and that BUN BUNSS was the submissive partner. In this manner, DAVIS remembered that BUN BUNSS would ask SCHAKEL if she could post something to the chat site and only SCHAKEL could give her permission to do so.

26. DAVIS said that SCHAKEL communicated to BUN BUNSS that they would eventually like her to come to Ohio. DAVIS planned to open his own trucking company and SCHAKEL would serve as his Information Technology Specialist. DAVIS explained that he and SCHAKEL wanted BUN BUNSS to work for them once his business was established. DAVIS and SCHAKEL discussed the possibility of engaging in sexual activity with BUN BUNSS once she was their employee. DAVIS said that he and SCHAKEL were going to travel to BUN BUNS'S residence, pick her up, and transport her to Ohio. DAVIS and SCHAKEL planned to travel to BUN BUNSS' residence via tractor-trailer. DAVIS articulated that the tractor-trailer would have a bed in it for DAVIS and BUN BUNSS. DAVIS implied that DAVIS and BUN BUNSS would engage in sexual activity, in the bed, while traveling to Ohio.

27. On April 12, 2023, in jail for the aforementioned parole violation, SCHAKEL telephoned his mother, KATHRYN. During the phone call, SCHAKEL asked KATHRYN if law

enforcement had already taken the server. KATHRYN responded they had not, indicating her knowledge of the whereabouts and status of the server. During the same call, KATHRYN advised SCHAKEL that he should invest in a program that would check identification of users on his server. SCHAKEL stated that he did not have enough users to justify that cost right now, but that he offered MV access to his server when she was having issues with a public server. SCHAKEL also stated that he wished he knew MV's actual age sooner.

28. Also on April 12, 2023, SCHAKEL telephonically contacted an associate, JACKSON WINGEIER[4] (hereinafter WINGEIER), whom SCHAKEL addressed as "Thorn." WINGEIER identified himself as SCHAKEL's "service provider." In the first conversation with WINGEIER after SCHAKEL's imprisonment, WINGEIER read SCHAKEL a list of official announcements. WINGEIER pronounced that SCHAKEL's services were currently terminated due to an active legal strike on SCHAKEL's account. The data were currently retained in an unusable state. All of SCHAKEL's machines were preserved but were not being powered on without further notice, and that, upon being released from incarceration, SCHAKEL has a defined number of days to ensure anybody that accesses his system is age verified.

29. In the same conversation, SCHAKEL and WINGEIER discussed the backup schedule that SCHAKEL had implemented for his server. WINGEIER expressed concern that SCHAKEL's backup schedule could potentially overwrite data on the server. Neither

[4] While attempting locate MV, the FBI interviewed Wingeier. Wingeier stated that he did not know MV's location, but provided additional information regarding Element and its functionality.

man elaborated on the location of the backup. WINGEIER stated that he needed to get to SCHAKEL's mom in order to access the server and change the backup schedule so data was not overwritten. WINGEIER also stated that SCHAKEL's mom was willing to freeze that backup as long as they could get her into the server. One method of how SCHAKEL's mother could access the server was through SCHAKEL's computer which had a different password than the server. WINGEIER wondered about KATHRYN'S ability to write various commands or perform various actions on the server.

30. During an April 23, 2023 jail call between SCHAKEL and KATHRYN, SCHAKEL explained that his laptop would be necessary for KATHRYN to access the server. KATHRYN replied that it would have to wait until she got the table cleared off [5].

31. Your Affiant avers that this conversation along with the reference to the laptop in paragraph 30 demonstrates that KATHRYN not only is aware of where the server is located, but also already has access to it and the other "computer." Investigators who met with KATHRYN on the day of SCHAKEL's arrest described her mobility as severely limited and possibly homebound indicating to the Affiant that only devices located within her dwelling would be physically accessible to her.

[5] The interior condition of SUBJECT PREMISES and most surface areas reflect the occupants to either be hoarders or physically unable to maintain a sanitary and uncluttered home.

CONCLUSION

32. Based on the foregoing facts, Affiant has probable cause to believe that SUBJECT PREMISES may contain evidence pertaining to those directly involved with the transportation of minor with the intent to engage in criminal sexual activity, coercion and enticement, and knowingly possessing child pornography.

Respectfully submitted,

Preetham C. Rao
Special Agent
Federal Bureau of Investigation

This affidavit was sworn to by the affiant by telephone
after a PDF was transmitted by email,
per Crim. R. 41(d)(3),
on this 1st day of May, 2023 at 2:34 p.m.

JENNIFER DOWDELL ARMSTRONG
UNITED STATES MAGISTRATE JUDGE